AMENDMENTS TO THE CLAIMS

1.   (Currently amended) A method of analyzing security events, comprising:

receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;

causing display[[ing]] of a graph on a display of a computer system, the graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and

causing display[[ing]], in conjunction with the graph, of security incident information[[,]] including causing display, with respect to a group device symbol, [[an]]of a security incident volume indicator that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol.

2.   (Currently amended) The method of claim 1, including

upon user selection of a group device symbol for a group of non-security devices, causing display[[ing]] of a second level graph on the display of the computer system, the second level graph representing the non-security devices in the group and the security devices in association with the group, the displayed second level graph including a plurality of non-security device symbols and a plurality of security device symbols, each non-security device symbol representing one non-security device in the group and each security device symbol representing one security device in the group; and

causing display[[ing]], in conjunction with the second level graph, of security incident information, including causing display, with respect to a non-security device symbol, [[an]]of a security incident volume indicator that indicates a number of network sessions whose source or destination is at the non-security device.

3.   (Currently amended) The method of claim 1, including

upon user command with respect to a user specified device symbol in the displayed

graph, causing display[[ing]] of data representing network sessions whose source

or destination is at a device corresponding to the user specified device symbol.

4.   (Original) The method of claim 3, including in response to one or more user commands,
selecting a network session from the displayed data, and defining a drop rule that comprises a set
of network conditions corresponding to the selected network session;

wherein the processing of security events includes filtering out network sessions that

satisfy the defined drop rule.

5.   (Original) The method of claim 3, wherein the data representing network sessions
includes source and destination identifying information, event type information indicating one or
more types of incidents corresponding to the network sessions, and security device information
indicating one or more security devices that report security events in association with the
network sessions.

6.   (Currently amended) The method of claim 1, wherein the processing of security events
includes identifying groups of network sessions that together satisfy a security incident
identification rule in a group of predefined security incident identification rules, and identifying
as rule firing network sessions each of the network sessions that is a member of any identified
group of network sessions;

wherein each security incident volume indicator indicates a number of rule firing network

sessions whose source or destination is at a device corresponding to the device

symbol.

7.   (Original) The method of claim 6, wherein the processing of security events includes
excluding from the rule firing network sessions any network session that satisfies any drop rule
in a set of drop rules, each drop rule defining a respective set of conditions.

8-15.   (Canceled)

16.   (Currently amended) A method of analyzing a stream of security events, comprising:

receiving and processing a stream of security events, including grouping the security events into a plurality of network sessions, each session having an identified source and destination and assigned a unique session identifier;

applying a plurality of predefined security event correlation rules to the plurality of network sessions in association with the processed security events;

for each of a subset of the predefined security event correlation rules, identifying network sessions from the plurality of network sessions in association with the processed security events, if any, that satisfy the rule;

causing display[[ing]] of a graph on a display of a computer system, the graph representing devices in a network, the displayed graph including a plurality of individual device symbols and a plurality of group device symbols, each individual device symbol representing one security device of the network, and each group device symbol representing a group of non-security devices of the network; and

causing display[[ing]], in conjunction with the graph, of information associated with the identified network sessions, including causing display, with respect to each group device symbol, of a session volume indicator that indicates a number of identified network sessions whose source or destination is at a non-security device in a group of non-security devices corresponding to the group device symbol.

17.   (Canceled)

18.   (Currently amended) A network security events analysis system, comprising:

one or more central processing units for executing programs;

an interface for receiving security events; and

a network security event correlation engine executable by the one or more central processing units, the engine comprising: instructions for receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;

instructions for causing display[[ing]] of a graph on a display of a computer system, the graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual

device symbols and a plurality of group device symbols, each individual device

symbol representing a security device of the network and each group device

symbol representing a group of non-security devices of the network; and

instructions for <u>causing</u> display[[ing]], in conjunction with the graph, of security incident

information, including <u>causing display,</u> with respect to a group device symbol,

[[an]]<u>of a security</u> incident volume indicator that indicates a number of network

sessions whose source or destination is at one member of a group of non-security

devices corresponding to the group device symbol.

19.   (Currently amended) The system of claim 18, including

instructions, respons<u>ive</u> to user selection of a group device symbol for a group of non-

security devices, for <u>causing</u> display[[ing]] <u>of</u> a second level graph <u>on the display</u>

<u>of the computer system, the second level graph</u> representing the non-security

devices in the group and the security devices in association with the group, the

displayed second level graph including a plurality of non-security device symbols

and a plurality of security device symbols, each non-security device symbol

representing one non-security device in the group and each security device

symbol representing one security device in the group; and

instructions for <u>causing</u> display[[ing]], in conjunction with the second level graph, of

security incident information, including <u>causing display,</u> with respect to a non-

security device symbol, [[an]]<u>of a security</u> incident volume indicator that

indicates a number of network sessions whose source or destination is at the non-

security device.

20.   (Currently amended) The system of claim 18, including

instructions, responsive to a user command with respect to a user specified device symbol

in the displayed graph, for <u>causing</u> display[[ing]] <u>of</u> data representing network

sessions whose source or destination is at a device corresponding to the user

specified device symbol.

21.   (Original) The system of claim 20, including instructions, responsive to one or more user

commands, for selecting a network session from the displayed data, and defining a drop rule that

comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

22.   (Original) The system of claim 20, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

23.   (Currently amended) The system of claim 18, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each security incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

24.   (Original) The system of claim 23, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.

25.   (Currently amended) A computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:
    instructions for receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;
    instructions for causing display[[ing]] of a graph on a display of a computer system, the graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual

device symbols and a plurality of group device symbols, each individual device

symbol representing a security device of the network and each group device

symbol representing a group of non-security devices of the network; and

instructions for causing display[[ing]], in conjunction with the graph, of security incident

information, including causing display, with respect to a group device symbol,

[[an]]of a security incident volume indicator that indicates a number of network

sessions whose source or destination is at one member of a group of non-security

devices corresponding to the group device symbol.

26.   (Currently amended) The computer program product of claim 25, including

instructions, responsive to user selection of a group device symbol for a group of non-

security devices, for causing display[[ing]] of a second level graph on the display

of the computer system, the second level graph representing the non-security

devices in the group and the security devices in association with the group, the

displayed second level graph including a plurality of non-security device symbols

and a plurality of security device symbols, each non-security device symbol

representing one non-security device in the group and each security device

symbol representing one security device in the group; and

instructions for causing display[[ing]], in conjunction with the second level graph, of

security incident information, including causing display, with respect to a non-

security device symbol, [[an]]of a security incident volume indicator that

indicates a number of network sessions whose source or destination is at the non-

security device.

27.   (Currently amended) The computer program product of claim 25, including

instructions, responsive to a user command with respect to a user specified device symbol

in the displayed graph, for causing display[[ing]] of data representing network

sessions whose source or destination is at a device corresponding to the user

specified device symbol.

28.   (Original) The computer program product of claim 27, including instructions, responsive

to one or more user commands, for selecting a network session from the displayed data, and

defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule.

29.   (Original) The computer program product of claim 27, wherein the data representing network sessions includes source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions.

30.   (Currently amended) The computer program product of claim 25, wherein the processing of security events includes identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each security incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol.

31.   (Original) The computer program product of claim 30, wherein the processing of security events includes excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions.